

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ANDREA GLADSTONE, individually and
on behalf of all others similarly situated,

Plaintiff,

v.

AMAZON WEB SERVICES, INC.,

Defendant.

CASE NO. 2:23-cv-00491-TL

ORDER ON MOTION TO DISMISS

This is an action for statutory damages under the California Invasion of Privacy Act (“CIPA”) for a software provider’s alleged unlawful access to and recording of telephone conversations between a bank and its customers. This matter is before the Court on Defendant Amazon Web Services, Inc.’s Rule 12(b)(6) Motion to Dismiss Second Amended Class Action Complaint. Dkt. No. 21. Having reviewed Plaintiff Andrea Gladstone’s response (Dkt. No. 24), Defendant’s reply (Dkt. No. 27), the Parties’ supplemental authorities (Dkt. Nos. 30–33, 39), and the relevant record, and having heard oral argument (Dkt. No. 43), the Court DENIES the motion.

I. BACKGROUND

Plaintiff is a citizen of California and a resident of Los Angeles County, California. Dkt. No. 18 ¶ 7. Defendant is a Delaware limited liability company with its principal place of business in Seattle, Washington. *Id.* ¶ 8.

A. Defendant's Service

Defendant offers a service called “Amazon Connect” with features that record and analyze callers’ voice and conversations. Dkt. No. 18 ¶ 8. Amazon Connect is “a machine-learning powered contact center service” for use in customer service departments, among others.¹ *Id.* ¶ 1; *see also id.* ¶ 17. It helps customer service agents provide personalized service, track and manage customer issues, and automatically search across connected repositories based on phrases and questions that customers ask. *Id.*; *see also id.* ¶¶ 18–19. For example, the “Contact Lens” feature enables search of analyzed and transcribed recordings based on the speaker, keywords, sentiment score, non-talk time for calls, and response time for chats. *Id.* ¶ 20.

When Amazon Connect is used, “[Defendant] itself is collecting the content of any conversation before said data is provided” to a customer like Capital One. *Id.* ¶ 25. Defendant also has the capability to access and analyze the data it collects through Amazon Connect to service its customers. *Id.* Customers can enable the service to record and analyze calls before the call begins, such that the recording and analysis are done contemporaneously with the conversation. *Id.* ¶ 27; *see also id.* ¶ 26 (diagram). Likewise, when a call is completed, customers

¹ Defendant asks the Court to consider portions of Defendant’s website related to Amazon Connect, as well as Defendant’s Service Terms, in the Court’s analysis. *See* Dkt. No. 21 at 10; Dkt. Nos. 22-1, 22-2, 22-3. Plaintiff does not appear to object. Accordingly, the Court considers these materials. *See Eugster v. Wash. State Bar Ass’n*, No. C15-375, 2015 WL 5175722, at *1 n.3 (W.D. Wash. Sept. 3, 2015) (“At the motion to dismiss stage, the court may properly treat a website quoted and cited in the complaint as incorporated by reference.”).

are provided with a recording and transcription of the call, along with details like customer sentiment analysis or customer-vs-agent talk time. *Id.* ¶ 28.

In its Service Terms, Defendant states that it can “use information about how [customers] use and interact with the Services to improve those services.” *Id.* ¶ 29 (quoting Service Terms ¶ 1.20). Defendant also states that customers can “request that Amazon Connect record an applicable audio session along with chat and other types of recordings.” *Id.* (quoting Service Terms ¶ 54.5). Further, customers agree that Defendant:

may use and store Amazon Connect ML Content to maintain and provide Amazon Connect ML Services (including development and improvement of Amazon Connect ML Services and their underlying technologies); . . . may use and store Amazon Connect ML Content that is not personal data to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and . . . solely in connection with the development and improvement described [above] . . . may store your Amazon Connect ML Content in AWS regions outside the AWS regions where you are using Amazon Connect ML Services.

Id. (quoting Service Terms ¶ 54.7(a)).

B. Plaintiff’s Experience

Plaintiff is a customer of Capital One. Dkt. No. 18 ¶ 35. Capital One uses Amazon Connect in its banking and fraud operations.² *Id.* ¶ 2. It uses the service to manage and monitor the telephone lines that its banking customers in California and across the country call to receive support. *Id.* ¶ 3. Amazon Connect is used on calls between Capital One and consumers, “through which Defendant records, gains access to, and otherwise reads, attempts to read, or learns the contents of conversations” that are collected. *Id.* ¶ 30. Capital One does not inform callers that Amazon Connect is being used, nor does it obtain consent for its use. *Id.* ¶¶ 31–32. When

² Defendant features Capital One as a “case study” on its website. *See Capital One Contact Centers Innovate Faster Using Amazon Connect*, Amazon Web Servs. (2018), <https://aws.amazon.com/solutions/case-studies/capital-one-amazon-connect> [<https://perma.cc/LBP4-PUXS>].

1 Defendant provided Amazon Connect to Capital One, “it was [Defendant’s] intention to record
2 the confidential communications of Capital One’s customers.” *Id.* ¶ 33.

3 In the year before filing her complaint, Plaintiff placed several calls from California to
4 Capital One’s Customer Support Center. *Id.* ¶ 36–37. Plaintiff alleges that she “reasonably
5 expected her conversations with Capital One to be confidential and only between [herself] and
6 Capital One (and any entities that Capital One directed her inquiry to).” *Id.* ¶ 38. Plaintiff further
7 alleges that “[t]hese conversations were with a banking entity, which naturally involves the
8 discussion of confidential information.” *Id.* Plaintiff called on her personal telephone and out of
9 the direct presence of others. *Id.*

10 During one call in or about October 2022, Plaintiff called Capital One to inquire as to
11 how to transfer funds from one account to another and to obtain a trust certification form. *Id.*
12 ¶ 39. In another call around the same time, Plaintiff called Capital One to initiate a partial refund
13 using her travel insurance. *Id.* ¶ 40. In another call around approximately March 2022, Plaintiff
14 called Capital One to inquire about an electronic transfer. *Id.* ¶ 41. During all these calls, Plaintiff
15 was asked to make “yes” or “no” statements to questions, or to provide additional information.
16 *Id.* ¶ 42. Unknown to her, her calls were “captured, recorded, accessed, and read by [Defendant]
17 through the Amazon Connect service,” while she was on the phone with Capital One. *Id.* ¶ 43.
18 Plaintiff did not give her consent for this activity prior to the call, either to Capital One or to
19 Defendant directly. *Id.* ¶¶ 44–45.

20 C. Procedural History

21 On March 31, 2023, Plaintiff commenced this action. Dkt. No. 1; *see also* Dkt. No. 18
22 (Second Amended Complaint (“SAC”)). Plaintiff asserts claims under CIPA for damages. Dkt.
23 No. 18 ¶¶ 5–6, 56–77. Plaintiff proposes a class of all California residents who had their
24 conversations recorded by Defendant using Amazon Connect, as well as a subclass of all

1 California residents who had their conversations with Capital One recorded by the same. Dkt.
2 No. 18 ¶¶ 47–48. Defendant now moves to dismiss the SAC. Dkt. No. 21; *see also* Dkt. No. 27
3 (reply). Plaintiff opposes. Dkt. No. 24; *see also* Dkt. Nos. 30–33, 39 (supplemental authorities).
4 On June 13, 2024, the Court heard oral argument on the motion. Dkt. No. 43.

5 II. LEGAL STANDARD

6 A defendant may seek dismissal when a plaintiff fails to state a claim upon which relief
7 can be granted. Fed. R. Civ. P. 12(b)(6). In reviewing a Rule 12(b)(6) motion to dismiss, the
8 Court takes all well-pleaded factual allegations as true and considers whether the complaint
9 “state[s] a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678
10 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While “[t]hreadbare
11 recitals of the elements of a cause of action, supported by mere conclusory statements” are
12 insufficient, a claim has “facial plausibility” when the party seeking relief “pleads factual content
13 that allows the court to draw the reasonable inference that the defendant is liable for the
14 misconduct alleged.” *Iqbal*, 556 U.S. at 672. “When reviewing a dismissal pursuant to
15 Rule . . . 12(b)(6), ‘we accept as true all facts alleged in the complaint and construe them in the
16 light most favorable to plaintiff[], the non-moving party.’” *DaVinci Aircraft, Inc. v. United*
17 *States*, 926 F.3d 1117, 1122 (9th Cir. 2019) (alteration in original) (quoting *Snyder & Assocs.*
18 *Acquisitions LLC v. United States*, 859 F.3d 1152, 1156–57 (9th Cir. 2017)).

19 III. DISCUSSION

20 “A federal court interpreting a state statute follows that state’s rules of statutory
21 construction.” *Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1132 (N.D. Cal. 2015)
22 (citing *Turnacliiff v. Westly*, 546 F.3d 1113, 1117 (9th Cir. 2008)); *accord In re Google Location*
23 *Hist. Litig.*, 428 F. Supp. 3d 185, 193 (N.D. Cal. 2019). In a recent CIPA case, the California
24 Supreme Court rearticulated some general principles of statutory interpretation:

“““When we interpret a statute, ‘[o]ur fundamental task ... is to determine the Legislature's intent so as to effectuate the law's purpose. We first examine the statutory language, giving it a plain and commonsense meaning. We do not examine that language in isolation, but in the context of the statutory framework as a whole in order to determine its scope and purpose and to harmonize the various parts of the enactment. If the language is clear, courts must generally follow its plain meaning unless a literal interpretation would result in absurd consequences the Legislature did not intend. If the statutory language permits more than one reasonable interpretation, courts may consider other aids, such as the statute's purpose, legislative history, and public policy.’ [Citation.] ‘Furthermore, we consider portions of a statute in the context of the entire statute and the statutory scheme of which it is a part, giving significance to every word, phrase, sentence, and part of an act in pursuance of the legislative purpose.’”””

Smith v. LoanMe, Inc., 483 P.3d 869, 872 (Cal. 2021) (alteration in original) (quoting *Meza v. Portfolio Recovery Assocs., LLC*, 434 P.3d 564, 570–71 (Cal. 2019)); *see also Kight v. CashCall, Inc.*, 133 Cal. Rptr. 3d 450, 455 (Cal. Ct. App. 2011).

“In 1967, the Legislature enacted [CIPA] to address concerns that ‘advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.’”

CashCall, 133 Cal. Rptr. 3d at 455–56 (quoting Cal. Penal Code § 630). “The purpose of the act was to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation.” *Smith*, 483 P.3d at 872–73 (quoting *Flanagan v. Flanagan*, 41 P.3d 575, 577 (2002)). Moreover, “the California Supreme Court has also emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA.” *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *2 (9th Cir. May

31, 2022) (first citing *Ribas v. Clark*, 696 P.2d 637, 639–41 (Cal. 1985); then citing *Smith*, 483 P.3d at 879).

A. Application of Section 631 to Defendant

CIPA Section 631 states in relevant part:

Any person [1] who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [4] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable

Cal. Penal Code § 631(a); *see also* Cal. Penal Code § 637.2 (authorizing private right of action under CIPA). The statute thus details “three distinct and mutually independent patterns of conduct: intentional wiretapping, wilfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities.” *Tavernetti v. Superior Ct.*, 583 P.2d 737, 741 (Cal. 1978).

Plaintiff appears to premise Defendant’s liability on the first two clauses of Section 631. *See* Dkt. No. 18 ¶¶ 62–63. Defendant argues that it is exempt from Section 631 liability because it falls under the “party exemption” to the statute (Dkt. No. 21 at 15–20), labeled by Plaintiff as the “extension” approach to third-party liability (Dkt. No. 24 at 13-15). Plaintiff responds that

1 Defendant is liable under two alternative approaches to third-party liability, which it labels the
2 “separate entity” and “capability” approaches. *Id.* at 7–13.

3 It is well established that a person who is a “party” to a communication is exempt from
4 Section 631(a) liability. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th
5 Cir. 2020) (citing *Warden v. Kahn*, 160 Cal. Rptr. 471, 475 (Cal. Ct. App. 1979)). However,
6 courts within the Ninth Circuit are split as to whether this exemption applies to a third party that
7 is hired by a party to a communication to do work for the party’s own benefit. *See Doe v. Kaiser*
8 *Found. Health Plan, Inc.*, No. C23-2865, 2024 WL 1589982, at *14–18 (N.D. Cal. Apr. 11,
9 2024) (reviewing leading approaches).

10 This divide traces back to a pair of California state court decisions to which courts
11 frequently analogize. In the first case, *Rogers v. Ulrich*, the plaintiff sued the City of San Jose
12 and a city employee who tape recorded portions of a telephone conversation between the plaintiff
13 and the employee. 125 Cal. Rptr. 306 (Cal. Ct. App. 1975). The court held that the employee was
14 *not* liable under Section 631 because the statute does not cover the recording of a conversation
15 made by a participant in the conversation. *Id.* at 308–09. As the court explained, “[i]t is never a
16 secret to one party to a conversation that the other party is listening to the conversation; only a
17 third party can listen secretly to a private conversation.” *Id.* at 309.

18 In the second case, *Ribas v. Clark*, the plaintiff sued a friend of his wife after the friend
19 listened in to a call between her and the plaintiff while the two were engaged in divorce
20 proceedings. 696 P.2d 637 (Cal. 1985). The court held that the wife’s friend *was* liable under
21 Section 631. *Id.* at 359–62. The court observed that “Section 631 was aimed at one aspect of the
22 privacy problem—eavesdropping, or the secret monitoring of conversations by third parties.” *Id.*
23 at 359. This problem includes “simultaneous dissemination to an unannounced second auditor.”
24 *Id.* at 360. “[I]t is probable,” the court added, “that the Legislature viewed Section 631 as a

means of proscribing attempts to circumvent other aspects of [CIPA], e.g., by requesting a secretary to secretly transcribe a conversation over an extension, rather than tape recording it in violation of section 632.” *Id.* at 631.

Thus, in recent years, courts of the Ninth Circuit have split in how they apply Section 631 at the pleading stage to software providers like Defendant. Some courts find that software providers are *not* third parties because they are a “extension” of their customers and merely “provide[] a tool”—like the tape recorder in *Rogers*—that allows a customer to carry out its own activities. *See, e.g., Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021).³ Other courts find software providers are third parties only when they have the “capability” to use customer data “for any other purpose (just as a tape recorder has no independent capability to divulge the recording for any other purpose but that of its owner).” *See, e.g., Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891 (N.D. Cal. 2023).⁴ A similar third (but smaller) group of courts appears to find software providers are *per se* third parties because they are “a separate legal entity”—like the wife’s friend in *Ribas*—and “not merely a passive device.” *See, e.g., Saleh v. Nike*, 562 F.

³ *Accord Williams v. What If Holdings, LLC*, No. C22-3780, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022); *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072 (C.D. Cal. 2023); *Williams v. DDR Media, LLC*, No. C22-3789, 2023 WL 5352896 (N.D. Cal. Aug. 18, 2023); *Licea v. Vitacost.com, Inc.*, 683 F. Supp. 3d 1118 (S.D. Cal. 2023); *Cody v. Boscov’s, Inc.*, 658 F. Supp. 3d 779 (C.D. Cal. 2023); *Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051 (C.D. Cal. 2023); *Martin v. Sephora USA Inc.*, No. C22-1355, 2023 WL 2717636 (E.D. Cal. Mar. 30, 2023), *report and recommendation adopted*, 2023 WL 306197 (Apr. 24, 2023); *Jones v. Peloton Interactive, Inc.*, No. C23-1082, 2024 WL 1123237 (S.D. Cal. Mar. 12, 2024).

⁴ *Accord Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073 (C.D. Cal. 2021); *Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962 (N.D. Cal. 2023); *Balletto v. Am. Honda Motor Co.*, No. C23-1018, 2023 WL 7026931 (N.D. Cal. Oct. 24, 2023); *Valenzuela v. Super Bright LEDs Inc.*, No. C23-1148, 2023 WL 8424472 (C.D. Cal. Nov. 27, 2023); *Cody v. Ring LLC*, No. C23-562, 2024 WL 735667 (N.D. Cal. Feb. 22, 2024); *Rodriguez v. Ford Motor Co.*, No. C23-598, 2024 WL 1223485 (S.D. Cal. Mar. 21, 2024); *D’Angelo v. FCA US LLC*, No. C23-982, 2024 WL 1625771 (S.D. Cal. Mar. 28, 2024); *Heiting v. Taro Pharmaceuticals USA, Inc.*, No. C23-8002, 2024 WL 1626114 (C.D. Cal. Apr. 2, 2024); *Turner v. Nuance Commc’ns, Inc.*, No. C22-5827, 2024 WL 2750017 (N.D. Cal. May 28, 2024).

1 Supp. 3d 503 (C.D. Cal. 2021).⁵ Finally, some courts have declined to take a firm position at the
 2 pleading stage, finding the allegations sufficient regardless. *See, e.g., Valenzuela v. Kroger Co.*,
 3 No. C22-6382, 2024 WL 1336959 (C.D. Cal. Mar. 28, 2024).⁶

4 Although the question is a close one, the Court “is persuaded by the reasoning in *Javier*,
 5 tracking a growing number of district courts which have reached the same conclusion.” *Turner*,
 6 2024 WL 2750017, at *10. In particular, the Court concurs with *Javier*’s critiques of *Graham*’s
 7 reading of Section 631—namely, (1) it interprets all of Section 631 “based on the intentions and
 8 usage of the prospective third party” when the third prong of Section 631 already contains a use
 9 requirement, and (2) it is contrary to *Ribas*, where the court “did not consider the wife’s friend’s
 10 intentions or the use to which they put the information they obtained.” *Javier*, 649 F. Supp. 3d at
 11 900. The Court also finds the *Saleh* approach (insofar as it offers an approach that is distinct
 12 from *Javier*, which Defendant disputes (*see* Dkt. No. 27 at 11–13)) too rigid, as the precise
 13 nature of a software provider is dependent on the facts of each case.

14 Applying the capability approach analysis, the Court finds that Plaintiff has sufficiently
 15 alleged a violation of Section 631. Defendant claims that the SAC does not allege that it had the
 16 capability to use Plaintiff’s communications for its own purpose, while simultaneously (and
 17 contradictorily) admitting that it “reserves its rights in the Service Terms to use certain customer
 18 information for service improvement . . . at the customers’ election and for *their* benefit.” Dkt.

19 ⁵ *Accord Revitch v. New Moosejaw*, No. C18-6827, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019); *Valenzuela v.*
 20 *Nationwide Mutual Ins. Co.*, 686 F. Supp. 3d 969 (C.D. Cal. Aug. 14, 2023); *D’Angelo v. Penny OpCo, LLC*,
 No. C23-981, 2023 WL 7006793 (S.D. Cal. Oct. 24, 2023).

21 ⁶ *Accord Doe v. Microsoft Corp.*, No. C23-718, 2023 WL 8780879 (W.D. Wash. Dec. 19, 2023); *Esparza v. UAG*
 22 *Escondido AI Inc.*, No. C23-102, 2024 WL 559241 (S.D. Cal. Feb. 12, 2024) (expressing sympathy for *Javier* and
 23 *Saleh* approaches but finding allegations sufficient even under *Graham* approach); *Smith v. Google LLC*, No. C23-
 24 3527, 2024 WL 2808270 (N.D. Cal. June 3, 2024) (finding allegations sufficient under either *Graham* or *Javier*
 approaches); *Rodriguez v. Aquatic Sales Solns. LLC*, No. C23-5198, 2024 WL 2804097 (May 29, 2024) (same);
Ahringer v. LoanDepot, Inc., No. C23-186, 2024 WL 1135683 (C.D. Cal. Feb. 6, 2024) (citing, *inter alia*, both
Javier and *Saleh* in finding allegations sufficient); *Garcia v. Yeti Coolers, LLC*, No. C23-2643, 2023 WL 5736006
 (C.D. Cal. Sept. 5, 2023) (same).

No. 27 at 10 (emphasis added). However, in its Service Terms—which Plaintiff cites in the SAC—Defendant states that it can “use information about how [customers] use and interact with the Services to improve those services.” Dkt. No. 18 ¶ 29 (quoting Service Terms ¶ 1.20). The SAC further alleges that customers like Capital One also agree that Defendant “may use and store Amazon Connect ML Content” to develop and improve *Defendant’s own* services. *Id.* (quoting Service Terms ¶ 54.7(a)). More generally, Plaintiff alleges that Defendant “is collecting the content of any conversation before said data is provided to any entity that was a party to the conversation (like Capital One),” and it “has the capability to analyze any data it collects through its Amazon Connect platform.” *Id.* At the very least, then, the Court can infer that Defendant can use the data it collects “to improve its own products and services,” which shows that it “is capable of creating, recording, and retaining” data for purposes other than sending the data back to Capital One. *Turner*, 2024 WL 2750017, at *10.

Defendant points out that its Customer Agreement⁷ states that Defendant “obtain[s] no rights” to a customer’s content except for use in providing services to the customer. *See* Dkt. No. 21 at 18 (quoting Dkt. No. 22-4 (agreement) ¶ 6.1). But as discussed above, the Court rejects an interpretation of Section 631 that is based on the intentions and usage of the software provider. Moreover, Plaintiff’s allegations demonstrate that Defendant has capabilities beyond that of a mere tape recorder, and there is no evidence that Defendant is incapable of using the data for any other purpose.⁸ *See, e.g.*, Dkt. No. 18 ¶¶ 18–19, 21–22, 24, 29; Dkt. No. 22-2; *cf.*

⁷ Defendant asks the Court to consider the AWS Customer Agreement, which is attached to the motion to dismiss. Dkt. No. 21 at 12 n.2. Plaintiff does not appear to object. *See generally* Dkt. No. 24. Accordingly, the Court will consider this material. *See Mayhall ex rel. D.M. v. Amazon Web Servs. Inc.*, No. C21-1473, 2022 WL 2718091, at *4 (May 24, 2022) (taking judicial notice because the Agreement “appear[s] on publicly available websites and the facts included are not subject to reasonable dispute”), *report and recommendation adopted*, 2023 WL 2728292 (Mar. 31, 2023).

⁸ Some courts that embrace the *Javier* approach take a more stringent view of what allegations are required to demonstrate a provider’s “capability to use” the data it collects.

1 *Smith*, 2024 WL 2808270, at *4 (suggesting that an online tracking service might “encrypt the
2 data it collects so that only the website developer, not the service provider, can access the
3 unencrypted data”).

4 Defendant also argues that its Service Terms are irrelevant because information about
5 customer “use” and “interact[ion]” are *not* content under CIPA, and because Plaintiff does not
6 allege that any machine-learning services were used in connection with her calls. *See* Dkt. No. 21
7 at 19–20; Dkt. No. 27 at 10. But Defendant admits (Dkt. No. 21 at 20; Dkt. No. 27 at 10) that
8 Plaintiff cannot allege these facts, as this would not be information typically available to or in the
9 control of a plaintiff. At this pre-discovery stage, Plaintiff (and the Court) cannot know what is
10 included in Defendant’s information about customer use or interaction, or whether machine-
11 learning services were used in relationship to her calls. Accepting Plaintiff’s allegations are true,
12 they are sufficient to survive the motion to dismiss.

13 **B. Application of Section 632 to Defendant**

14 CIPA Section 632 states in relevant part:

15 A person who, intentionally and without the consent of all parties to
16 a confidential communication, uses an electronic amplifying or
17 recording device to eavesdrop upon or record the confidential
18 communication, whether the communication is carried on among
19 the parties in the presence of one another or by means of a telegraph,
20 telephone, or other device, except a radio, shall be punished

21 Cal. Penal Code § 632(a). A “confidential communication” is further defined as

22 any communication carried on in circumstances as may reasonably
23 indicate that any party to the communication desires it to be
24 confined to the parties thereto, but excludes a communication
made in a public gathering or in any legislative, judicial, executive,
or administrative proceeding open to the public, or in any other
circumstance in which the parties to the communication may
reasonably expect that the communication may be overheard or
recorded.

1 Cal. Penal Code § 632(c). Defendant argues that it is exempt from Section 632 liability for three
2 reasons. Dkt. No. 21 at 21–25. The Court considers each in turn.

3 **1. Whether Amazon Connect Is “Electronic Amplifying or Recording Device”**

4 Defendant argues that Amazon Connect is a software service, not “an electronic
5 amplifying or recording device.” Dkt. No. 21 at 21–22; Dkt. No. 27 at 15. Defendant argues that
6 traditional tools of statutory interpretation support a reading of the phrase that excludes a
7 software service and instead captures only tangible, physical devices. *Id.* In response, Plaintiff
8 points to courts that have interpreted analogous statutes, including the federal Wiretap Act, to
9 include software as a covered “device.” Dkt. No. 24 at 16–17. Defendant replies that the
10 language in CIPA is meaningfully distinguishable from other statutes. Dkt. No. 27 at 15.

11 CIPA does not define “device,” and few courts have squarely addressed the issue.
12 However, courts frequently look to the Wiretap Act when analyzing a CIPA claim. *See, e.g.,*
13 *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (“The analysis for a violation
14 of CIPA is the same as that under the federal Wiretap Act.” (quoting *Cline v. Reetz-Laiolo*, 329
15 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018))); *In re Facebook*, 956 F.3d at 607 (“Courts perform
16 the same analysis for both the Wiretap Act and CIPA regarding the party exemption.”).
17 Moreover, “[t]he majority of courts to consider this issue have entertained the notion that
18 software may be considered a device for purposes of the Wiretap Act.” *United States v.*
19 *Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) (gathering cases). To the Court’s eye, the
20 gravamen of these cases is that “device” is often understood in context—in particular, the
21 privacy context—to be more expansive than, say, “equipment” or “mechanism,” as Defendant’s
22 reliance on dictionary definitions (*see* Dkt. No. 21 at 21) would require. *See State of Cal. v. Altus*
23 *Finance*, 116 P.3d 1175, 1181 (Cal. 2005) (“To seek the meaning of a statute is not simply to
24 look up dictionary definitions and then stitch together the results. Rather, it is to discern the sense

1 of the statute, and therefore its words, *in the legal and broader culture*.” (emphasis in original)
2 (quoting *Hodges v. Superior Ct.*, 980 P.3d 433, 437 (Cal. 1999))).

3 In addition, the Ninth Circuit has observed the California Supreme Court’s instruction
4 that “all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory
5 purposes of CIPA.” *Javier*, 2022 WL 1744107, at *2. Plus, “[a]dvances in technology can
6 increase the potential for unreasonable intrusions into personal privacy.” *In re Facebook*, 956
7 F.3d at 599 (quoting *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019)). “[I]n an era
8 when millions of Americans conduct their affairs increasingly through electronic devices, the
9 assertion . . . that federal courts are powerless to provide a remedy when an internet company
10 surreptitiously collects private data . . . is untenable.” *Id.* (quoting *In re Google Inc. Cookie*
11 *Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019)).

12 With all these principles in mind, the Court finds that “device,” as used in Section 632,
13 can include software. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1080 (N.D. Cal.
14 2023) (holding the same); *cf. Rodriguez*, 2024 WL 1223485, at *7 (under Section 631(a), noting
15 it is “not apparent” why statutory term “machine” would apply to a computer “but not the
16 software that a computer entails”); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 (N.D. Cal.
17 2015) (under the Wiretap Act, holding complaint properly alleged software was an “[e]lectronic,
18 mechanical, or other device”).

19 Defendant points out that “device” is used a second time in Section 632, at the end of a
20 list of terms that cabin the meaning of “device.” *See* Dkt. No. 21 at 21–22; Cal. Penal Code
21 § 632(a) (“by means of a telegraph, telephone, or other device”). That is true as far as it goes—to
22 the meaning of “device” as used in that list of terms. *See People v. Drennan*, 101 Cal. Rptr. 2d
23 584, 588 (Cal. Ct. App. 2000) (explaining the interpretive canon of *noscitur a sociis*). But here,
24 “device” as used in “electronic amplifying or recording device” is not cabined in the same way

1 the second use of “device” is. And the California Supreme Court has cautioned against a robotic
2 application of the same meaning to the same word used in different contexts, even within the
3 same statute:

4 True: Courts often presume that a word used in more than one
5 provision of a statute has precisely the same meaning throughout –
6 – a logical inference rooted not only in how people ordinarily use
7 language, but also in how one generally might expect legislative
8 bodies to draft statutory provisions. Yet this is merely a
9 presumption, not an inflexible rule. Just as people sometimes use
10 the same word to convey different meanings even in the same
11 sentence, so too have we held that certain statutes are sometimes
12 best read in context to assign different meanings to the same word
13 used in different portions of a statute. Our interpretive task is not
14 necessarily to slavishly assign a word precisely the same meaning
15 every time it is used in a statute — regardless of the context — but
16 to accord it the meaning best suited to effectuating the statute's
17 intended purpose.

18 *People v. Superior Ct.*, 431 P.3d 141, 146 (Cal. 2018) (internal citations omitted); *cf. People v.*
19 *Gibbons*, 263 Cal. Rptr. 905, 907–08 (Cal. Ct. App. 1989) (“[I]n the text of section 630, no
20 reference is made to a specific device or instrument for eavesdropping. Rather, the prohibition is
21 based on the purpose for which the device or instrument is used.”).

22 Defendant also points out that Section 631 prohibits eavesdropping or recording “by
23 means of any machine, instrument, or contrivance, or in any other manner”—comparatively
24 broad language that suggests “device” in Section 632 should be interpreted more narrowly. *See*
Dkt. No. 21 at 22. To be sure, the use of “materially different language in statutory provisions
addressing the same subject or related subjects” gives rise to the “normal inference” that “the
Legislature intended a difference in meaning.” *People v. Trevino*, 27 P.3d 283, 285 (Cal. 2001).
But Section 631’s different language is not especially probative of how to define the contours of
“device” in Section 632. Put another way, the differences in language do not exclude the
possibility that Sections 631 and 632 can *both* apply to software, even if their scope differs.

To be sure, courts have read “device” more narrowly when context calls for it. For example, Section 637.7 defines “electronic tracking device” as “any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.” Cal. Penal Code § 637.7(d). Accordingly, courts have understood “device” in Section 637.7 to refer to equipment. *See, e.g., In re Google Location Hist. Litig.*, 428 F. Supp. 3d at 193. But Section 632 contains materially different language than Section 637.7, and it does not contain similar context that would narrow the meaning of “device” here.

2. Whether Defendant “Uses” Amazon Connect to Record or Eavesdrop

Defendant argues that it did not “use” Amazon Connect to record or eavesdrop on Plaintiff’s calls. Dkt. No. 21 at 23; Dkt. No. 27 at 16. Specifically, Defendant argues that it merely “enables *Capital One* and other customers to use Amazon Connect; [it] does not *use* Amazon Connect itself.” Dkt. No. 21 at 23 (emphases in original). Plaintiff responds that “once Capital One decides what benefits it would like to derive from Amazon Connect, it is Defendant who ‘uses’ the device.” Dkt. No. 24 at 18; *see id.* at 17–18. As with the term “device,” CIPA does not define what “use” means, though Defendant points out (Dkt. No. 21 at 23) that at least one dictionary⁹ defines the term to mean, among other things, “to put into action or service” or “to carry out a purpose or action by means of.” *Use*, Merriam-Webster Dictionary, <https://www.merriam-webster.com/dictionary/use> [<https://perma.cc/9NXA-W9UC>].

Here, the Court finds that Plaintiff sufficiently alleges that Defendant “uses” Amazon Connect. Plaintiff alleges that Defendant “itself is collecting the content of any conversation

⁹ It is not apparent why a current dictionary is a useful guide to the interpretation of a statute enacted decades ago. *See MCI Commc’ns Servs., Inc. v. Calif. Dep’t of Tax & Fee Admin.*, 239 Cal. Rptr. 3d 241, 247 (Cal. Ct. App. 2018) (“[R]elevant dictionary definitions are those extant before or at least near in time to the statutory or contractual usage.” (quoting *Siskiyou Cnty. Farm Bureau v. Dep’t of Fish & Wildlife*, 188 Cal. Rptr. 3d 141, 157 (Cal. Ct. App. 2015))). And again, determining the meaning of a statute is to discern the sense of the statute and its words “in the legal and broader culture.” *Altus Finance*, 116 P.3d at 1181.

before said data is provided” to customers. Dkt. No. 18 ¶ 25. “[W]hen an agent is listening to a conversation, [Defendant] is also listening simultaneously through Amazon Connect.” *Id.* ¶ 26. “[C]ustomers can enable [Defendant] to ‘record’ and ‘analyze’ calls before a call even begins, such that once a call starts, the recording and analyze [sic] is done contemporaneously with the conversation.” *Id.* ¶ 27. “[O]nce the call has completed, [Defendant] provides the recording and transcription of the call” *Id.* ¶ 28. Under a plain and commonsense understanding of the term “use,” the Court finds that these allegations are sufficient at this stage to establish that Defendant itself is a user of Amazon Connect, even if some use is ultimately at the direction of Capital One.

3. Whether Capital One Failed to Provide Notice of Call Recording and Whether Plaintiff’s Calls Were Confidential Communications

Finally, Defendant nominally argues that Plaintiff does not allege that Capital One failed to provide notice that her calls would be recorded. Dkt. No. 21 at 24–25; Dkt. No. 27 at 13–14. Defendant also appears to argue that Plaintiff did not allege facts to support a finding that her conversation with Capital One was a “confidential communication”—a distinct but related argument. *Id.* Plaintiff first responds that Defendant has the burden to establish consent to recording. Dkt. No. 24 at 18. Plaintiff further responds that Plaintiff alleges that she had a reasonable expectation of privacy in her call with Capital One. *Id.* at 19–21.

“A communication is ‘confidential’ . . . if a party to the conversation had an *objectively reasonable expectation* that the conversation was *not being overheard or recorded*.” *CashCall*, 133 Cal. Rptr. 3d at 462 (emphases in original) (citing *Flanagan*, 41 P.3d at 579–82). “The issue whether there exists a reasonable expectation that no one is secretly recording or listening to a phone conversation is generally a question of fact.” *Id.* (citing *Lieberman v. KCOP Television*,

1 *Inc.*, 1 Cal. Rptr. 3d 536, 545 (Cal. Ct. App. 2003)); *accord Santa Ana Police Off. Ass’n v. City*
 2 *of Santa Ana*, 219 Cal. Rptr. 3d 919, 924 (Cal. Ct. App. 2017).

3 Here, the Court finds that Plaintiff sufficiently alleges both that Capital One failed to
 4 provide notice that her calls would be recorded and that her calls were confidential
 5 communications. Plaintiff alleges that “[u]nbeknownst to her, when Plaintiff Gladstone called
 6 Capital One’s customer support center, her telephone conversation was captured, recorded,
 7 access, and read by [Defendant] Amazon.” Dkt. No. 18 ¶ 43 (emphasis added). She also alleges
 8 that “Capital One did not procure [her] consent” to recording her calls. *Id.* ¶ 44. While Plaintiff’s
 9 allegations are not a model of clarity, there is no specific language required to make out
 10 sufficient allegations.

11 Moreover, Plaintiff alleges that she “reasonably expected her conversations with Capital
 12 One to be confidential” and provides summaries of the content of those conversations. *Id.* ¶ 38.
 13 For example, one call was about “how to transfer funds from one account to another and to
 14 obtain a trust certification form.” *Id.* ¶ 39. Another call was “to initiate a partial refund using her
 15 travel insurance, for a trip she was unable to take because of an injury.” *Id.* ¶ 40. Yet another call
 16 was “to inquire about an electronic transfer.” *Id.* ¶ 41. Bearing in mind that a person’s
 17 “objectively reasonable expectation” of confidentiality is “generally a question of fact,”
 18 *CashCall*, 133 Cal. Rptr. 3d at 462, the Court finds that these allegations of personal banking-
 19 related calls are more than sufficient to survive a motion to dismiss.

20 **C. Intentional or Willful Acts by Defendant**

21 Finally, Defendant argues that both of Plaintiff’s claims should be dismissed because she
 22 does not allege that Defendant acted intentionally or willfully, an element of both Section 631
 23 and Section 632 claims. *See* Dkt. No. 21 at 25–29. Specifically, Defendant argues that the SAC
 24 does not allege that Defendant intended to “record *any* communications, much less *confidential*

1 communications or *Ms. Gladstone's* confidential communications.” *Id.* at 27 (emphases in
2 original). Instead, “the SAC alleges only that [Defendant] fulfilled *Capital One's* intent by allow
3 capital One to use Amazon Connect to record the conversations of Capital One’s choosing.” *Id.*
4 (emphasis in original). Plaintiff responds that Defendant’s intent turns on disputed questions of
5 fact and that Amazon Connect is designed for the purpose of intercepting communications. Dkt.
6 No. 24 at 21–22. Defendant replies that “[k]nowing Amazon Connect’s capabilities and its
7 customers’ industries does not create substantial certainty that confidential communications will
8 be recorded.” Dkt. No. 27 at 16–17.

9 “[T]he recording of a confidential conversation is intentional if the person using the
10 recording equipment does so with the purpose or desire of recording a confidential conversation,
11 or *with the knowledge to a substantial certainty that his use of the equipment will result in the*
12 *recording of a confidential conversation.*” *Rojas v. HSBC Card Servs. Inc.*, 228 Cal. Rptr. 3d
13 640, 646 (Cal. Ct. App. 2018) (emphasis in original) (quoting *People v. Superior Ct. of Los*
14 *Angeles Cnty.* (“*Smith*”), 449 P.2d 230, 238 (Cal. 1969)). Whether a person possesses the
15 requisite intent under CIPA is generally a question of fact. *Id.* at 646 n.11 (citing *Smith*, 449 P.2d
16 at 238).

17 Here, the Court finds that Plaintiff has adequately pled that Defendant acted intentionally
18 and willfully. The SAC alleges that Amazon Connect is designed for the purpose of recording
19 and analyzing communications between its customers (like Capital One) and consumers or other
20 entities. *See, e.g.*, Dkt. No. 18 ¶¶ 18–28. Indeed, Defendant features Capital One as a “case
21 study” on its website, demonstrating specific awareness of the nature of Capital One’s business.
22 *Id.* ¶ 2 n.5. Defendant points out that it “contractually requires companies that use Amazon
23 Connect to provide notice and obtain consent from their customers” (Dkt. No. 21 at 28), but “the
24 Court is not convinced that [Defendant’s] inclusion of a catch-all provision requiring its

1 customers to comply with the law generally is enough to satisfy its legal obligations” under
2 CIPA. *Rivera v. Amazon Web Servs., Inc.*, No. C22-269, 2023 WL 4761481, at *10 (W.D. Wash.
3 July 26, 2023) (regarding a different privacy statute). Whether Defendant truly possessed the
4 requisite intent will be “tested on an evidentiary record.” *Doe*, 690 F. Supp. 3d at 1080.

5 IV. CONCLUSION

6 Accordingly, Defendant’s Rule 12(b)(6) Motion to Dismiss Second Amended Class
7 Action Complaint (Dkt. No. 21) is DENIED. Pursuant to the Court’s prior Order (Dkt. No. 29), the
8 Parties are reminded to meet and confer and propose a trial schedule **within fourteen (14) days**
9 of this Order.

10 Dated this 2nd day of July 2024.

11 
12 _____
13 Tana Lin
14 United States District Judge
15
16
17
18
19
20
21
22
23
24